Appl. No. : **09/755,452**
Filed : **January 5, 2001**

REMARKS

Reconsideration and allowance of the above-referenced application are respectfully requested.

Claims 1-27 stand rejected under 35 U.S.C. 102(e) as allegedly being anticipated by Tello. This contention, however, is respectfully traversed. (note that a minor change for clear antecedent basis has been made to claim 1.) Claim 1 defines a method where the user is identified using unique information, and a first plurality of files and computer are designated as being associated with that user. Responsive to that identifying, a program is used to allow the user to make a change to a first plurality of files associated with the user, and the contents of the first plurality of files cannot be read if the user is not identified.

This is a very different system than Tello. Tello teaches effectively using a smart card to restrict access to a computer. The smart card identification is admittedly carried out on the BIOS level. However, when the smart card is not identified, the computer is shut down securely. The computer may be prevented from booting. No device drivers will be loaded, and the computer is not operable, see generally column 5 lines 42-45. This is also discussed beginning column 9 which describes the enabling and disabling circuit that disables keyboard, parallel port, floppy drive, and IDE that drives the hard drive.

This is very different than the subject matter of claim 1. Specifically, the present claim 1 designates a first plurality of files on the computer as being associated with the user and uses a program to allow that user to make a change to those files associated

with the user. Nowhere does Tello in anyway teach or suggest designating any files as being associated with the user.

Certainly Tello does identify the user, and responsive to that identifying allows the user to make a change to any file on the whole computer. However, there is no teaching or suggestion of designating the files as being associated with the user as claimed. Claim 1 also requires preventing reading the contents of the files when the user is not identified. Tello prevents the computer from booting, so in that sense it might prevent reading the contents of the files. However, since the computer cannot boot, there is no way to "prevent" anything.

In any case, there is nothing in Tello, and certainly nothing in Tello's column 5 lines 15-48 which teaches "designating a first plurality of files in a computer as being associated with said user" as claimed. Therefore, claim 1 should be allowable along with the claims that depend therefrom.

Claim 5 teaches a very different feature, where there is a second plurality of files on the computer that are read only files. These files can be read, but no changes to these files are allowed. The rejection alleges that this is shown in Tello column 14 lines 24-27 and 40-45. Column 14 describes different levels of access, and says not much more than that. Lines 25-27 describes "different levels of access". Lines 40-41 describe that different storage devices may be encrypted. There is no teaching or suggestion, however, of designating a second plurality of files as read-only, not allowing a changes to those files, and those files being different than those which are identified as corresponding to the user.

Similarly, column 19 lines 40-45 teaches hiding restricted files. It teaches nothing about read-only files which are separate from the files that are associated with the user. Therefore, claim 1 should be additionally allowable for these reasons.

Claim 7 specifies security measures which allows special files to only be accessed via programs. This is not taught or suggested by the general statement in Tello that different levels of security can be granted. The subject matter of claims 6 and 7 allow a specified program to access certain files and nothing in Tello teaches anything about this.

Claim 10 has been amended to include the limitations of claim 11 therein. According to amended claim 10, both unencrypted and encrypted files are stored, with the unencrypted files in read-only, and the encrypted files in read/write files. This has the effect of preventing any kind of virus from infecting the computer, since the unencrypted files can only be read. Encrypted files are read/write, but these encrypted files can only be accessed with the proper decryption key. The rejection states that this is shown in column 14 lines 4-20. However, all the states is the different levels of access can be granted, it teaches nothing about unencrypted files in read-only and encrypted files being read/write.

The rejection alternately stakes that this is shown in Tello column 19 lines 44-55 which was discussed above. This simply states that restricted files can be hidden during repair and maintenance. Tello teaches nothing about encrypting read write files and leaving unencrypted files as read-only. Therefore, claim 10 should be allowable for these reasons.

Claim 13 specifies special files that are not read write files that are unencrypted, and again this is further allowable over the cited prior art for reasons discussed above.

Claim 14 specifies controlling files on the computer that prevents access to specified files but allows access to other files, unless unique information is used. As extensively discussed above, Tello is an all or nothing system. If the unique information is not used, booting is prevented. There is no access to any files.

Claim 15 is even further allowable, since it states that the access is allowed only to read-only files. Very little damage or on damage can be done using the read-only file. Without the specific unique information, access to read write files is prevented according to claim 15. This has been extensively discussed above, and nowhere is there any teaching or suggestion of this feature.

Claim 17 specifies that the access is controlled by encrypting the files. While admittedly Tello teaches encryption, and also teaches access control, it teaches nothing about using encryption as a method of access control, as claimed.

Claim 22 should be allowable for reasons discussed above. Nothing in Tello teaches or suggests "a first plurality of files in a computer, as being associated with said user...". Nothing the prior art teaches or suggests encrypting the files as a security mechanism, so that the user can not make changes to any of the files or read the files when the user is not identified. Nothing in the prior art teaches responsive to said identifying, using said operating system associated program in said computer to allow said user to make any changes to any of said first plurality of files using said encryption system associated with said user and to prevent reading contents of said first plurality of read/write files when said user is not identified;

allowing other unencrypted files on said system to be read when said user is not identified, but preventing writing to said other unencrypted files. Finally, nothing in the prior art teaches the special files which are encrypted but can be used only after another specified security operations.

Claim 23 teaches a system which "determines specified files on the computer system would qualify for a specified security aspect" and encrypting files other than those specified files using a unique code. As described above, Tello is an all or nothing system. It teaches nothing about differentiating the files in this way. Column 4 lines 15-48 teach preventing the device from booting if the user is not identified. It teaches nothing about encrypting all files other than those specified files using the unique code. Therefore, claim 23 should be additionally allowable.

This system has the unique advantage that only the user can view and/or change certain files. Someone other than the authorized user can still get certain kinds of access. For example, certain kinds of read-only files might be used to start a program such as Word (TM). However, even if the user can start that program, the user can not view or modify another user's personal information. This is not taught or suggested by Tello and the claims defining this feature should hence be allowable thereover.

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been

expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Therefore, and in view of the above amendments and remarks, all of the claim should be in condition for allowance. A formal notice to that effect is respectfully solicited.

Please charge any fees due in connection with this response to Deposit Account No. 50-1387.

Respectfully submitted,

Date: 10/12/04

Scott C. Harris
Reg. No. 32,030

Customer No. 23844
Scott C. Harris, Esq.
P.O. Box 927649
San Diego, CA 92192
Telephone: (619) 823-7778
Facsimile: (858) 678-5082